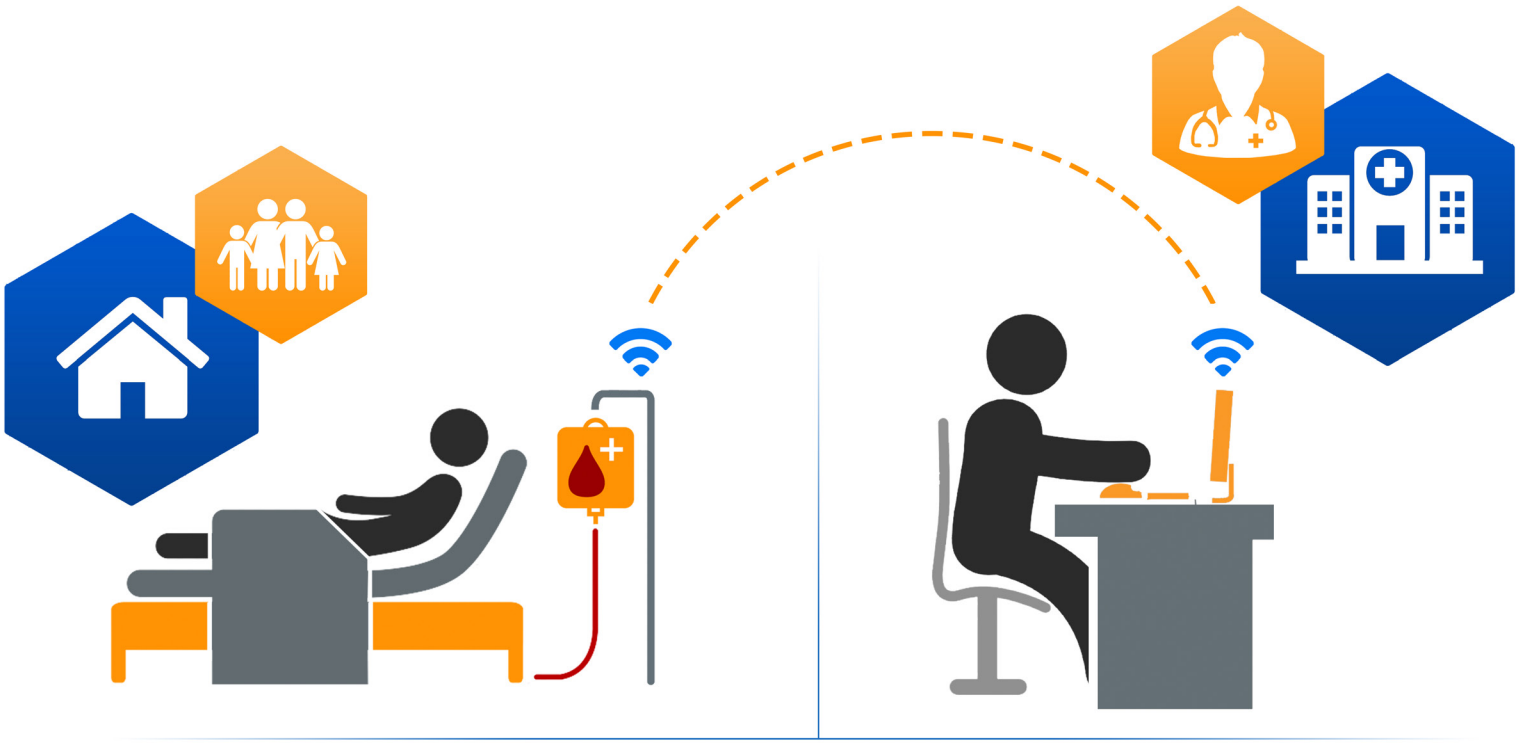
DEVICE AUTHORITY

ENTRUST

HEALTHCARE IOT SECURITY BLUEPRINT

REQUIREMENTS, COMPONENTS AND GUIDELINES



Introduction

The Internet of Things (IoT) presents a massive business opportunity across almost every industry. But to realize that opportunity, security must become a primary focus. If you cannot trust the data, there is no point in collecting, running analytics and executing decisions based on the data. IoT brings new security challenges introduced by the scale and pace of adoption, as well as the physical consequences of compromised security.

Until now, security has been treated as an afterthought; by adding layers of security after devices are delivered, with infrastructure and applications already in place. But security for the IoT, and the healthcare industry in particular, is too important to be treated as an afterthought. IoT's unique characteristics are forcing a fundamental rethink about how enterprises in general, and the healthcare sector in particular, need to implement security management for devices and the data.

Key Requirements for any IoT Security Solution

- Device and data security, including authentication of devices and confidentiality and integrity of data
- Implementing and running security operations at IoT scale
- Meeting compliance requirements and requests
- Meeting performance requirements as per the use case

Key Functional Blocks

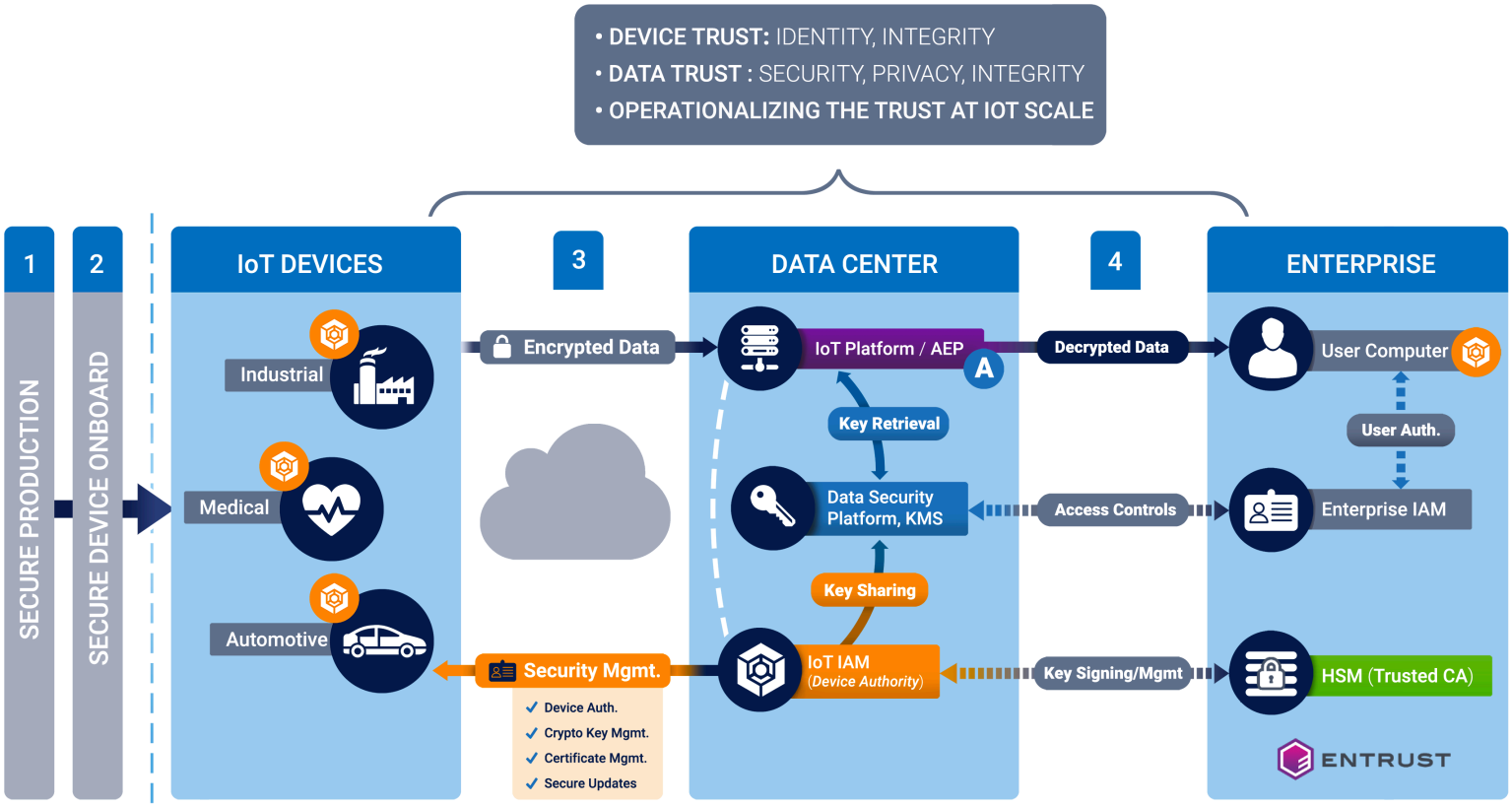
- Device Trust: Establishing and managing Device Identity and Integrity
- Data Trust: Policy driven end-to-end data security, privacy from creation to consumption
- Operationalizing the Trust: Automating and interfacing to the standards based, proven technologies/ products. E.g. PKI products

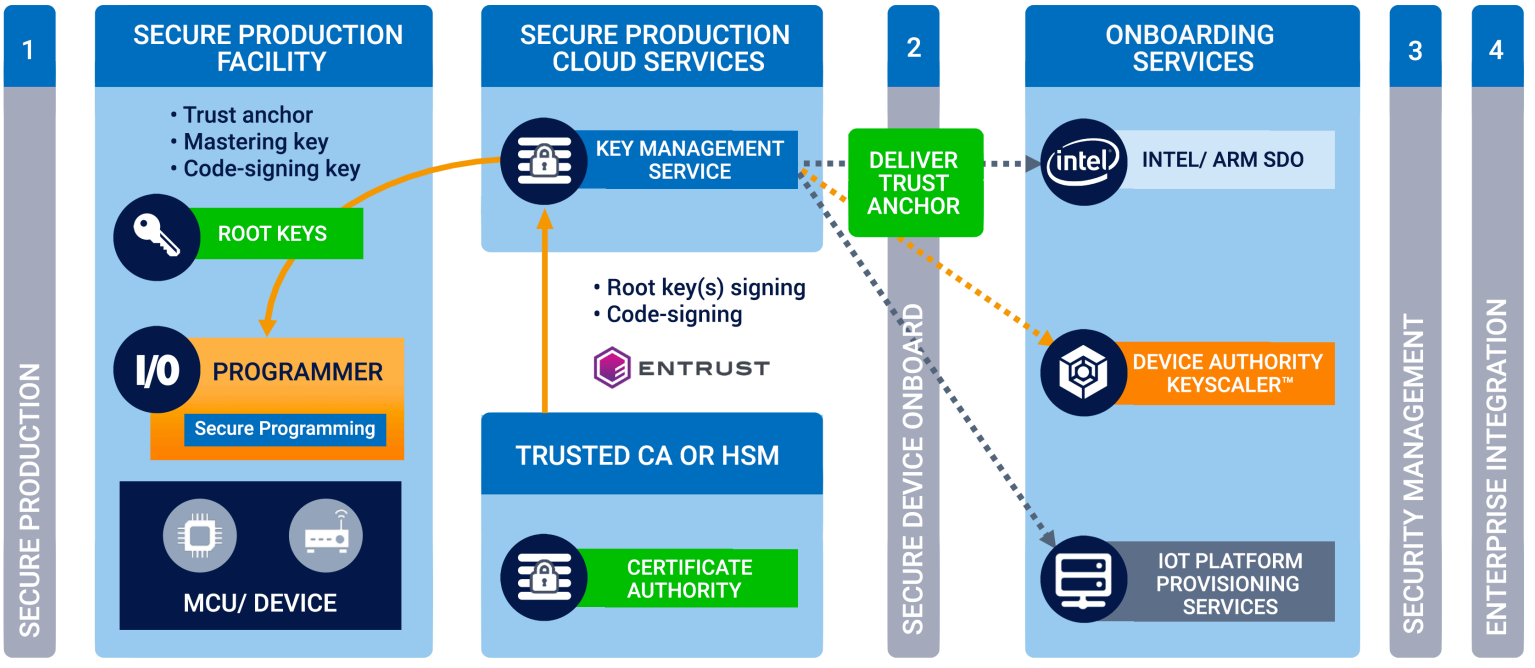
Note: IoT security solutions need to implement the above functional blocks as interconnected modules, not in isolation in order to meet the IoT scale, data security, device trust and compliance requirements.

Implementation Level Flows and Details

Function	Description	Core value
Provision root keys, trust anchor early in device lifecycle (e.g. at the time of manufacturing)	Provision immutable trust for devices at the time of manufacturing or before registering for secure device on boarding at IoT scale without human intervention	• Device Trust • Zero touch provisioning • Secure Updates
Registering, onboarding the devices into IoT platform and applications	The trust anchor and whitelisting based approach to register, provision and update devices through active, policy-based security controls that do not require human intervention	• Device Identity/Authentication • Eliminate rogue devices (cloned and counterfeit devices) • IoT Scale
Establish owner/app required security and manage as per the policy	Provision and manage identity, authentication and crypto keys as per the application requirements. This might involve interfacing to third party products and services. E.g. private or public Certificate Authority for device certificate signing	• Protect IoT application and Data • Operational management / efficiency
Policy driven end-to-end data encryption	Secure data exchange between IoT devices, IoT applications and resources including patients and clinicians	• Data security and privacy • Compliance
Policy driven authorization for applications and users	Only authorized applications access secrets on the device and authorized users access the data. Data at rest is stored encrypted and unreadable to unauthorized entities	• Data security and privacy • Compliance

Healthcare IoT Security Solution Blueprint





There are four main steps in this IoT Security solution

1. Provision Root Keys and Certificates at the Time of Manufacturing: Existing security solutions evolved as an afterthought. The potential impact of IoT security breach is forcing the right security model from the design and manufacturing phase. There are initiatives from government and standards bodies to promote "Secure by Design". This step establishes the foundation for secure devices from manufacturing.

- Provision strong "Root of Trust" and keys / certificates as required
- Root key and other device parameters like serial number act as registration information (whitelisting). In an ideal scenario, registration keys are rotated with a new key at the time of onboarding the device
- Secure mastering, production and foundation for secure updates need to be included in this step

2. Secure Device Onboard/Zero Touch Provisioning: Today's manual processes do not work well for IoT devices, scale and security. This is a new step that is required to transfer the ownership and connect to an owner-controlled environment without human intervention. Prominent vendors like Intel and Microsoft have initiated this type of implementation to help IoT security and adoption.

- Automated onboarding, ownership transfer leveraging the trust anchor and registration information
- Initial device configuration for interaction with IoT IAM or Security Management system

3. Provision and Manage Owner-Controlled Security for the Devices: This functionality is delivered by Device Identity centric IAM platforms like Device Authority's KeyScaler. This step is also new for IoT. While there are some home-grown implementations by platform vendors, many industry experts and analysts have talked about the functionality as IoT IAM, substantially different from traditional IAM.

- Provision and manage owner/application required keys and/or credentials
- Provision and manage application required identity/authentication
- Policy based automation for identity, authentication and data security keys

4. Integration: The majority of IoT security implementations need to take existing IT security controls into account and seamlessly interoperate with IoT devices. The challenge here is the correct integration of IoT IAM with the traditional Enterprise IAM, Hardware Security Modules (HSMs) and Data Security Platforms.

- HSMs like the Entrust nShield®, provide a Root of Trust, secure storage of keys, and secure crypto operations. HSMs are used for IoT identity provisioning and data security operations
- Healthcare organizations use data security platforms for key management and policy based data access authorization. Integration with these systems is essential for end-to-end data security and compliance. This is required for secure data exchange between IoT devices, other resources such as databases and patients and clinicians

- IoT IAM and Enterprise traditional IAM need to interoperate to authorize and share data between IoT devices, other resources and patients and clinicians

Operationalizing the Trust at IoT Scale

Many of the above steps are important and new for IoT security solutions. Today, a manual process exists where devices are activated in the field, configured on the network by IT, and registered with the device owner in an IoT management platform. This time-intensive process is fraught with security holes, as exemplified by recent large-scale attacks in which device manufacturers have shipped default credentials that were co-opted for botnet-style DNS attacks. Intel, Microsoft and many platform vendors have announced different approaches for some of these steps.

Device Authority's KeyScaler platform plays a major role in these steps by allowing organizations to automate and deliver owner-controlled security posture as per the IoT platform/application requirements and also integrate with the IT security infrastructure. KeyScaler enables healthcare organizations to become IoT ready, by allowing them to leverage IoT Application Enablement Platforms (AEPs) and use Certificate Authorities (CAs) and HSMs for security operations.

Root of Trust

Certificate signing and encryption keys underpin the security of an IoT system. Keys handled outside the protected cryptographic boundary of an HSM are significantly more vulnerable to attack, which can lead to compromise of critical keys. HSMs are the only proven and auditable way to secure valuable cryptographic material. Entrust nShield HSMs secure the generation and storage of the private keys used by the KeyScaler platform within a FIPS 140-2 Level 3 and Common Criteria EAL4+ certified environment. Doing so provides the highest level of security and assurance against key compromise and theft.

Conclusion

Existing security solutions have evolved as an afterthought for the changing digital world. We now have an opportunity to include security earlier at the design stage, in the new IoT world.

Device identity and integrity are the new perimeter for IoT. Data security and privacy are extremely important to healthcare IoT use cases. Any IoT security solution requires a combination of automated PKI, high assurance PKI key storage and management, along with enterprise data security platform integration. The implementation needs to be Device Identity centric. The modules need to work in unison, not as isolated devices, in order to meet data security and compliance requirements.

Device Authority and its partner Entrust have developed this blueprint architecture for mission critical healthcare IoT use cases, including diagnostics, treatment and monitoring. Many use cases require an IoT IAM platform which provides the 'glue' to extend security from the Enterprise to IoT devices.

About Entrust

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

To find out more about Entrust solutions for data encryption, multi-cloud key management and workload security visit entrust.com/HSM

Trust for every Thing

Device Authority is a global leader in Identity and Access Management (IAM) for the Internet of Things (IoT); focused on medical / healthcare, industrial and smart connected devices. Our KeyScaler™ platform provides trust for IoT devices and the IoT ecosystem, to address the challenges of securing the Internet of Things. KeyScaler uses breakthrough technology including Dynamic Device Key Generation (DDKG) and PKI Signature+ that delivers unrivalled simplicity and trust to IoT devices. This solution delivers automated device provisioning, authentication, credential management and policy based end-to-end data security/encryption.

With offices in California, USA and Reading, UK, Device Authority partners with leading IoT ecosystem providers.

Keep updated by visiting www.deviceauthority.com, following @DeviceAuthority on Twitter and subscribing to our BrightTALK channel.

DEVICE AUTHORITY™

sales@deviceauthority.com

www.deviceauthority.com

UK Head Office
Level 2 - Fora,
Thames Tower,
Station Road,
Reading, RG1 1LX